DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

The Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senator Wyden:

Thank you for your letter of June 27, 2013, regarding the Intelligence Community's use of section 215 of the USA PATRIOT Act, 50 U.S.C. § 1861, to obtain telephony metadata from U.S. service providers. In light of our desire to be transparent with the public about these activities to the extent consistent with national security, I will provide as much information as I can in this unclassified response, which will be accompanied by a classified supplement.

We are in agreement that it is highly unfortunate that the collection of telephony metadata was revealed through an unauthorized disclosure of classified information. This leak, along with the others that have occurred, will do significant damage to the Intelligence Community's ability to protect the nation. But it is not correct to say that Section 215 had been "secretly reinterpreted." The relevant materials were, of course, properly classified to protect sensitive intelligence collection activity, but, as Congress required, the Executive Branch fully and repeatedly briefed the Intelligence and Judiciary Committees of both Houses about the program and timely provided copies of the relevant classified documents to the Committees. Moreover, the Executive Branch undertook special efforts to ensure that all Members of Congress had access to information regarding this classified program prior to the USA PATRIOT Act's reauthorization in 2011, including making a detailed classified white paper available to all Members. Specifically, in December 2009, the Department of Justice and the Intelligence Community provided a classified briefing paper to the Senate and House Intelligence Committees that could be made available to all Members of Congress regarding the telephony metadata program. Both Intelligence Committees made this document available to all Members prior to the February 2010 reauthorization of Section 215. That briefing paper was then updated and provided to the Senate and House Intelligence Committees again in February 2011 for all Members in connection with the reauthorization that occurred later that year.

The data collected under this program is limited to telephony metadata: information about telephone calls such as the originating and dialed telephone numbers, the time a call is made and its duration. It does <u>not</u> include the content of any communication or the identity of any party to a communication. As you correctly note, the Supreme Court has squarely held that this type of information is not protected by the Fourth Amendment. In addition, as we have repeatedly and publicly said, we are <u>not</u> collecting cell site location information under this program. On October 20, 2011 the Director of the National Security Agency (DIRNSA) committed to the Senate Select Committee on Intelligence that he would notify Congress if NSA intended in the future to obtain cell site location information <u>prior</u> to doing so. As you know, DIRNSA reiterated this commitment before the Committee on 25 June 2013.

Senator Ron Wyden

Even though the Fourth Amendment is not implicated by the Government's acquisition of telephony metadata, we recognize there are sensitivities about the program that stem from the volume of records collected, which is why the program is subject to significant safeguards within and outside the Executive Branch. First, the Intelligence Community acquires telephony metadata as part of its overall efforts to protect the nation from terrorist threats, not to enable broad brush surveillance of the American public. Data acquired under this program may be used only to discover whether known or suspected terrorists have been in contact with other persons who may be engaged in terrorist activities. Second, queries of the data must be based on a documented, reasonable, articulable suspicion that the phone number used to query the database is associated with one of the terrorist entities specifically listed on the order of the Foreign Intelligence Surveillance Court (FISC). The vast majority of the data is never viewed by any person because it is not responsive to the limited, terrorism-related queries that are authorized. Third, the raw records may only be retained for up to five years. Finally, dissemination of query results may occur only if certain specific conditions imposed by the FISC are met.

We agree with you that, in order to ensure appropriate protection of privacy and civil liberties, these rules must be accompanied by strict oversight. That is why we have an extensive and multi-layered program to oversee compliance, involving all three branches of Government. The FISC must find that the proposed collection, and the procedures used to implement the program, are consistent with the law. And, of course, the collection and the procedures must comport with the Constitution. Data collected under this program is kept in secure databases and only specially trained personnel have access to it. Implementation of the program is regularly reviewed not only by NSA, but by outside lawyers from the Department of Justice and by my office, as well as by Inspectors General. The Executive Branch reports all compliance incidents on to the FISC. More detailed information about this program, and its oversight, is available in the public statements my office has released and in the record of the public hearing held before the House Permanent Select Committee on Intelligence.

With the above context in mind, I am able to answer the following questions without revealing additional classified national security information. As noted, additional information is provided in a classified annex.

(1) "How long has the NSA used PATRIOT Act authorities to engage in bulk collection of Americans' records? Was this collection underway when the law was reauthorized in 2006?"

NSA first began obtaining telephony metadata pursuant to Section 215 of the Patriot Act, as described above, in May of 2006. As you are aware, the FISA Court reviews and reauthorizes this program approximately every 90 days. In addition, this program was operational and, as discussed above, Congress was fully aware of it when it reauthorized the legislation for an additional five year period in 2011. Additional information is provided in the classified supplement.

(2) "Has the NSA used USA PATRIOT Act authorities to conduct bulk collection of any other types of records pertaining to Americans, beyond phone records?"

In addition to the bulk telephony metadata collection, NSA has in the past used FISA authorities to collect bulk Internet metadata. The Government terminated this collection program in 2011 for operational and resource reasons as reflected in the classified December 2, 2011 letter to the Senate Select Committee on Intelligence. NSA has not used USA PATRIOT Act authorities to conduct bulk collection of any other types of records. Additional information is provided in the classified supplement.

(3) "Has the NSA collected or made any plans to collect Americans' cell-site location data in bulk?"

As noted above, under this program NSA is not currently receiving cell site location data, and has no current plans to do so. The Director of NSA indicated on October 20, 2011 that he would notify Congress of NSA's intent to obtain cell site location data prior to any such plans being put in place. This commitment was reaffirmed again on June 25, 2013 before the Committee. Additional information is provided in the classified supplement.

(4) "Have there been any violations of the court orders permitting this bulk collection, or of the rules governing access to these records? If so, please describe these violations."

The collection and analysis of telephony metadata is a complex program and is subject to safeguards and controls that are designed and monitored through NSA's internal mission compliance program. NSA's compliance efforts, in turn, are subject to internal and external oversight. These safeguards and controls provide reasonable assurance that NSA's activities are consistent with law and policy and help detect when mistakes do occur, as they inevitably do in activities this complex, whether in the government or private sector. Since the telephony metadata collection program under section 215 was initiated, there have been a number of compliance problems that have been previously identified and detailed in reports to the Court and briefings to Congress as a result of Department of Justice reviews and internal NSA oversight. However, there have been no findings of any intentional or bad-faith violations.

These problems generally involved human error or highly sophisticated technology issues related to NSA's compliance with particular aspects of the Court's orders. As required, these matters, including details and appropriate internal remedial actions, are reported to NSA's Inspector General, the Department of Justice, the Office of the Director of National Intelligence, the FISC and in reports provided to Congress and other oversight organizations.

We are willing to provide you with additional information or further descriptions of these previously identified matters in a classified setting.

(5) "Please identify any specific examples of instances in which intelligence gained by reviewing phone records obtained through Section 215 bulk collection proved useful in thwarting a particular terrorist plot."

We have previously declassified two instances where the Section 215 bulk collection was useful: the attempt by Najibullah Zazi to bomb the New York subway system, and the material support investigation of Basaaly Moalim. Other examples which have already been provided and which must remain classified for operational reasons are provided in the classified supplement.

(6) "Please provide specific examples of instances in which useful intelligence was gained by reviewing phone records that could not have been obtained without the bulk collection authority, if such examples exist."

Please see the classified response to this question.

(7) "Please provide the employment status of all persons with conceivable access to this data, including IT professionals, and detail whether they are federal employees, civilian or military, or contractors."

Specific information regarding the composition of the Intelligence Community workforce that identifies resources dedicated to an intelligence objective is classified. Please see the classified response to this question.

Thank you for your continued interest in this topic. I hope this information has been helpful, and I look forward to our continuing discussions.

Sincerely,

James R. Clapper

Enclosure: Can be viewed in Senate Select Committee on Intelligence office spaces.